Journal of Computers Vol. 28, No. 5, 2017, pp. 155-161
doi:10.3966/199115992017102805014

LBS Privacy Preserving Model and Security Analysis Based on Expanded Anonymous Server

Peng-shou Xie[12], Tian-xia Fu[1], Jia Guo[1] and Qi Wang[1]

[1] School of Computer and Communications, Lanzhou University of Technology,
287 Langongping Road, Lanzhou, Gansu 730050, China
xiepsh_lut@163.com, 1142926852@qq.com

[2] Research Center of Engineering and Technology for Manufacturing Informatization of Gansu Province,
287 Langongping Road, Lanzhou, Gansu 730050, China
xiepsh_lut@163.com

Received 6 June 2016; Revised 7 February 2017; Accepted 8 February 2017

Abstract. Considering the existence of privacy security threats in LBS, we designed a Expanded Anonymous Server based on traditional LBS system structure to protect privacy information. It use the fully homomorphic encryption method to ensure the safety of Anonymous Server; At the same time, the onion algorithm and asymmetric encryption methods are used to design an improved LBS privacy preserving model based on expanded anonymous server. The model ensures the user's information is guaranteed to be not tampered or leaked. Using attack algorithm to detect the LBS preserving model and traditional LBS model, the security analysis shows that LBS preserving model can protect the user's anonymous identity, location information and service content effectively in LBS.

Keywords: anonymous communication, data encryption, location based service, privacy preserving

1 Introduction

Location based services refers to the cooperation through mobile terminals and network to determine the actual place of the mobile users, and to provide mobile applications with the location information, so which can achieve various services that are related to the user's Location. The existing LBS service system consists of three parts: Basic user terminal, Anonymous server and LBS server. However, the existing research is based on the hypothesis that the anonymous device is safe and reliable. And at present the reliability of the anonymous apparatus has not been proved. In addition, the LBS awareness within IoT (Internet of Things) space is very complicated. For example, one user's information may contain identity information, motion trail, behaviors and living habits and so on. Compared with the LBS system based on Internet, the LBS system within IoT space is facing more serious privacy issues. To solve above problems, many researchers have put forward to some relevant solutions.

A trajectory privacy model was proposed in the paper [1]. The model of [1] by formalizing an Adversary Model and defining weak trajectory privacy and strong trajectory privacy to effectively analyze and find the privacy vulnerabilities of RFID security protocols. Paper [2] based on Secure Multi-Party computation [3] to protect the privacy of IoT environment security. Paper [4] put forward a kind of safe and efficient scheme that used fuzzy key word to query; the scheme implemented the cloud data fuzzy keywords query, while maintaining the confidentiality of the query key words. Paper [5] put forward to a secure multi-keyword ranked search scheme over encrypted cloud data, which simultaneously supports dynamic update operations like deletion and insertion of documents. A self-destruction system, named CloudSky, was proposed in Paper [6]. This is able to enforce the security of user privacy over the untrusted cloud. CloudSky exploits a key control mechanism based on the attribute-based encryption (ABE) and takes advantage of active storage networks to allow the user to control the subjective life-cycle. Paper [7] presented a location privacy protection model based on the central server

structure. This scheme has been proven to achieve a blind query and perfect anonymous.

2 The Expanded Anonymous Server

Existing LBS system is mostly based on Anonymous Server, and the existing research is under the assumption that Anonymous Server itself is reliable. However, there is no authority certificate to prove the reliability of the Anonymous Server. Once the anonymous device is attacked successfully, the user's privacy will get a serious threat. Thus, extending the Anonymous Server in LBS system, making it safe and reliable is our first-line work.

LBS privacy security model includes the mobile user terminals, the expanded Anonymous Server and a LBS Service Provider. Its process is: Users sent its position information, query information and privacy requirements k to the Anonymous Server; Anonymous Server extend the user's precise location to be a anonymous area including other k-1 the users according to the privacy requirements of users [8]; Then sent the region and the user's query request to LBS Service Provider, after get the result set, Anonymous Server according to the location of the users to calculate the accurate results and select the accurate results from the result set which meeting the demand of users queries, and then return the query to user. The expanded anonymous server structure in this paper is shown in Fig. 1. That includes Anonymous Computing Center (ab. ACC), Encryption Center (ab. EC), Knowledge Base (ab. KB), and Query Result Refine Processor (ab. Q-RR).

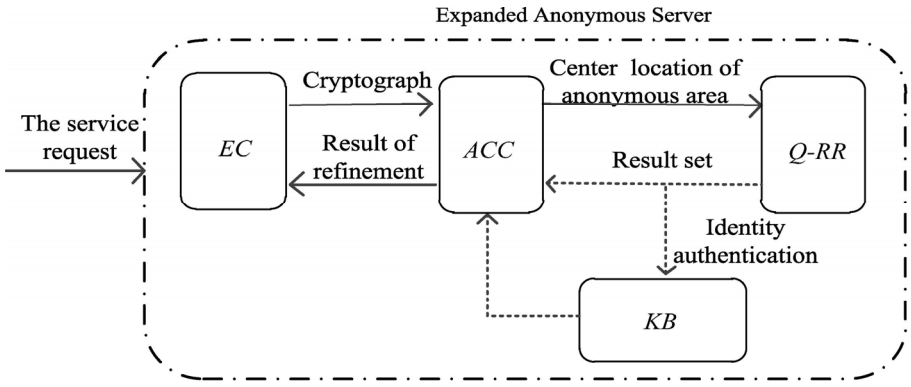

Fig. 1. Structure of the Expanded Anonymous Server

2.1 Encryption Center (EC)

The service request contains much information such as user's personal information, location information, user's request, user's privacy requirement parameters k and required minimum acreage of anonymous area and so on. All above of information are so important that should not be leaked. Thus the Encryption Center is responsible for encrypting the user's information and location information, and storing them in Knowledge Base. The encrypt process as shown in Fig. 2.

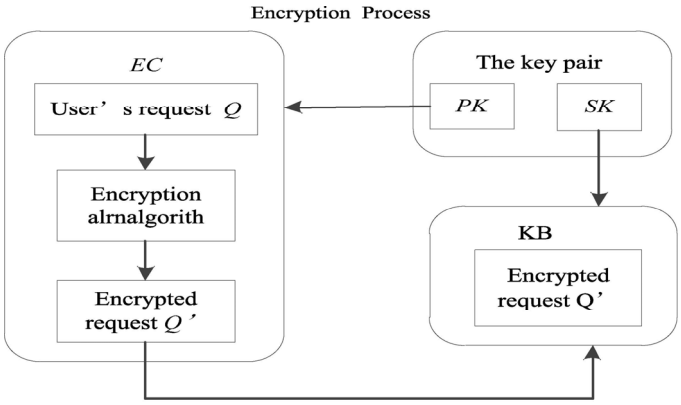

Fig. 2. Schematic diagram of the encrypting process

Users sent the service request Q to Anonymous Server, then Knowledge Base generates the public key (ab. PK) and private key (ab. SK); Encryption Center uses the PK to encrypt Q to be Q' and then stores it in Knowledge Base; Knowledge Base has saved the SK and will not decode it but directly store cryptograph Q'; In the result refine processing phase, the Query Result Refine Processor will filter the result sets according to the user's service requests and his true location in Knowledge Base[8]. At this point, the Query Result Refine Processor makes a request to the Knowledge Base. Knowledge Base will make an identity authentication for it, only after it passes the identity authentication. Knowledge Base will use SK to decode the Q' and sent to Query Result Refine Processor.

The date encryption process is as follows:

1. Choosing two classified distinct large prime numbers p and q, calculate their product M = p * q, then select a appropriate size safety parameters t, which has the greatest common divisor 1 with n, namely the GCD (t, n) = l, and then make the SK is d, PK is collection {e, t}.
2. Encryption center uses public key PK to encrypt Q, the encryption transformation as follows,

$$Q' = E(Q) = (Q + t * e) \bmod M. \quad \textbf{(1)}$$

3. The Knowledge Base uses the private key SK to decrypt the ciphertext Q' to the following change,

$$Q = D(Q') = Q' \bmod d. \quad \textbf{(2)}$$

2.2 Knowledge Base (KB)

Using KB to store information that users has sent and candidate set of query results. The service request information Q includes that user's personal information, location information, service contents and so on. These information will be anonymous in the Anonymous Device, so we need to preserve them locally. After get the query results set, LBS Server will return the results set to Anonymous Server for refining. Therefore, we also need to save the information, and the Knowledge Base is used to save the information.

2.3 Anonymous Computing Center (ACC)

Anonymous Computing Center (ACC) accords user's requirements to generate the anonymous area [9]. According to the regional selection algorithm and privacy requirements k, Anonymous Computing Center will calculate the acreage of the anonymous area to meet the user's required minimum anonymous area acreage. Anonymous computing center will find the center of the area and send it to LBS server according to the information provided by the user, and store them in Knowledge Base at the same time.

2.4 Query Result Refine Processor (Q-RR)

The returned result by Expanded Anonymous server is not a specific result but a result set. Query Result Refine Processor will save the set firstly, and then refine the result set according to the user's service requests and the true location of the user stored in Knowledge Base, and then send the refined result to the user, at the same time, the query result refinement processor will save the query result set. In case of the next time user sends the same service request. The query result refinement processor can return the results directly.

According to the Fig. 2, the Knowledge Base does not save user's service request Q, rather than encrypts service request Q'. When LBS server sending query result sets to the Anonymous Server, the KB holds the query result set. At this point, the Refine Processor needs to refine the collection, and the refine processor will send an authentication to the KB. After receiving the authentication, KB will search this authentication in its own database, if the authentication is effective, that is, the Knowledge Base itself has saved the authentication, the KB will decrypt Q' by using its private key SK and then send decrypted information only to the Refine Processor, and it will refine the information. In this way, inside the Anonymous Server, the processing of user's service request is transparent. The attacker cannot obtain relevant information about the user from Anonymity Server. By this way the safety of the Anonymity Server itself is ensured.

3 LBS Privacy preserving Model Based on Expanded Anonymous Server

After Anonymous Computing Center getting the anonymous area, it will store the anonymous information in the Knowledge Base, and then send information to the LBS server. LBS server includes the sender and the receiver. The contents that Anonymity Server sent to the LBS server are anonymity area and user's service requests. Which have been treated by ACC does not contain user's personal information. Therefore, transmission between LBS server does not need to use complex data encryption algorithm.

Having studied the existing literature and algorithm, the transmission between LBS server is proposed to use the anonymous communication technologies. Paper [10] pointed out anonymous communication hides the information of receiver and the sender's network address, communication relations, identification and other sensitive information in network communications, thus the eavesdropper cannot directly obtain or infer clear information of communicating parties. So the anonymous communication technologies can realize information sender anonymity, information receiver anonymity, communication relations anonymity between entities, location anonymity (inability to identify the location of the information sender and the receiver, mobile information, route information and topology information) etc. So LBS Privacy preserving Model Based on Expanded Anonymous Server can realize the data transmission and the safety of the classified data communication privacy preserving.

LBS security model is shown in Fig. 3.

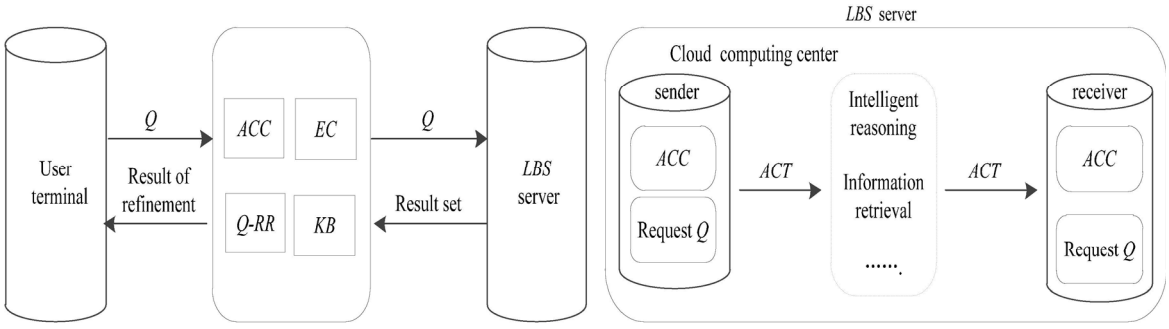

Fig. 3. LBS privacy security model

The existing anonymous communication algorithm mainly includes the MIX [11], Onion Routing algorithm [12] and flooding algorithm [13].The Onion Routing algorithm is used to pay attention to the real-time data communication and the effectiveness and practicability of the anonymous system. It conformed to the requirement of LBS server communication. Therefore, this model based on the algorithm to realize the communication of sensory data and location information. Onion routing is based on the channel to realize the data message transmission. So we need multiple nodes to establish channel, subsequent data transmitted through the channel in turn. Having studied the existing literature and algorithm, the transmission between LBS server using the Anonymous Communication Technologies (ACT) and the Onion routing algorithm to realize the communication of sensory data and location information is proposed. The LBS privacy preserving model which using Onion Routing algorithm need three phases: establish a channel, packet generation and transfer, release the channel.

Communication processes between different nodes is shown in Fig. 4 .

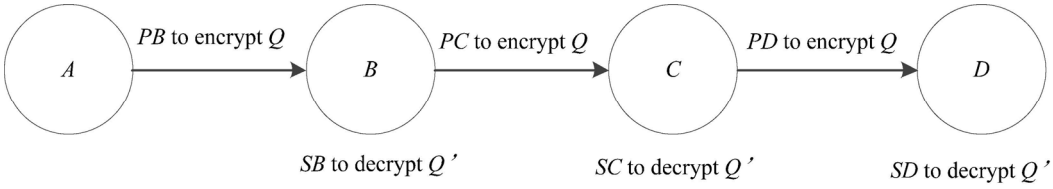

Fig. 4. Encryption process of the Anonymous communications

Step 1. Establishment of the communication channel: the establishment of channel needs three nodes at least. Assume that there are four nodes A, B, C, D. With B and C as intermediate proxy node that need to use the anonymous agent, node A sends the message, node D receives the message. Nodes A, D according to the routing information get the information of next communication nodes, thus creating a safe anonymous communication link. Each intermediate node is responsible for the asymmetric encryption and decryption of the message Q and encryption anonymous communication nodes by the private key.

Step 2. Packet generation and transmission: the first packet needs to establish a secure communication channel and the subsequent packets just need to along the channel to transmit, the last packet need to release the channel. Before sending, packets need to get the next jump through node's public key PK. For example, node A sends a packet Q to node B. Well first, using the PB, which is generated by node B, to encrypt Q into Q', at the same time save the PB; then sending Q' to B. After receiving Q', B will use its own private key SB to decode Q' into Q, and then continue using the public key PC, which is generated by node C, to encrypt Q and then send it to C, and so on. Node A keeps a counter k to record the number of packets.

Step 3. Release the communication channel: When counter k recording to the last packet, node A will send out the last packet at the same time reset k=0 and delete the PB. Also, after send the last packet, node B and C will delete the private key which node B and C have kept.

So, according to Fig. 3 and Fig. 4, LBS privacy preserving model based on expanded anonymous server can practicability protect private information with the use of anonymous communication mechanism between LBS servers and asymmetric encryption mechanism between different nodes data transmission.

4 Security Analysis

The proposed LBS model based on the expanded anonymous device is compared with the traditional LBS model in [14], in which the central server only anonymously handles the information sent by users. Using Baidu LBS cloud development platform [15] to build a foundation of LBS service Lab, Network based Generator of Moving Objects [16] to simulate the trajectories of users in the urban traffic network, and the traffic network graph of German Oden Berg as the simulation program input. The number of users is 500-2000, the speed of the user is 5-50km/h, average speed is 15km/h, query number of species N=2*103, anonymous cycles τ is 30s. The average time per user is 200τ, the range of the searching anonymity set is 2000*2000 m2 and the number of queries is about 2 *104.

Use attack algorithm that aimed at LBS continuous queries proposed in paper [17] to attack the two comparative models, and use success rate of attacks E, i.e., ratio of the number of queries that are successfully identified by the real sender and the number of all queries to judge the performance of the model. The experimental results are shown below in Fig. 5. According to the Fig. 5, when k value is same and take the value between15 and 40, the success rate of attacks of LBS model based on the expanded anonymous is lower than Traditional LBS model about 10 percent. It suggests that, LBS model based on the expanded anonymous can decrease the identified ratio of useful information by the attacker and the degree of protection of the user's privacy get improved under the equal conditions. Thus, LBS model based on the expanded anonymous have better privacy preserving effect compared to traditional LBS model.

Use the attack algorithm (CQACA) proposed in paper [18] and typical continuous query attack algorithm Clique Cloaking [19] to compare the two models. And using the error rate E between the user's motion captured by attack algorithm and the actual trajectory to measure the effectiveness of the two models, the experimental results are shown in Fig. 6. As can be seen from the Fig. 6, the error rate of LBS model based on the expanded anonymous is greater than Traditional LBS model when using the same algorithm to attack the models at the same time. It shows that LBS model based on the expanded anonymous can effectively protect the user's location information. At the same time, we can see that the fluctuation of error rate with the time is very small according to the Fig. 6. In fact, the average value of the error rate can be calculated on the basis of the formula which proposed by paper [18-19]. The mean values of the error rates of CQACA attacks on the two models are 11.44% and 16.92% respectively. The average error rates of the Cloaking Clique attacks are 17.23% and 19.37% respectively.

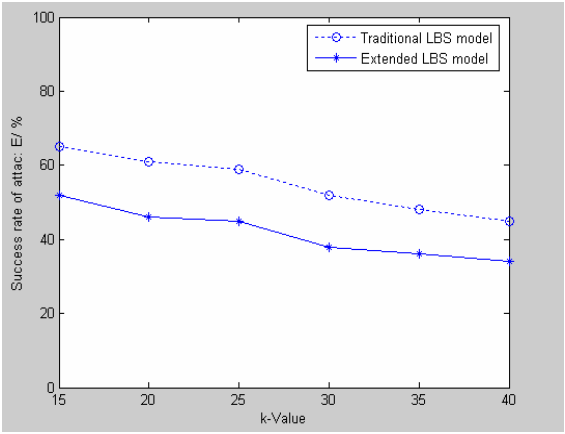

Fig. 5. Success rate of attacks of periodic queries

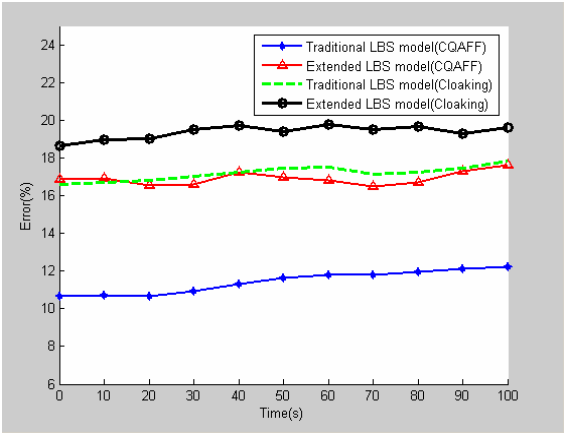

Fig. 6. Contrast of two models using two attack algorithms

As the Fig. 6 shows that when the attacker received the information with high error rate, user privacy can be better protected. It's demonstrates the reasonableness of the conclusion in Fig. 5. Under the same conditions, LBS model based on the expanded anonymous can decrease the identified ratio of useful information by the attacker.

5 Conclusion

Through analyzing the problems of existing LBS service framework and using encryption algorithm extends the traditional Anonymous Server to ensure its own security. At the same time, using anonymous communication to design LBS privacy preserving model based on expanded Anonymous Server ensure the user's information is guaranteed to be not tampered or leaked. This model can effectively protect the safety of users' privacy in LBS service. However, the expanded anonymous used the encryption mechanism, which affects the speed of service, increases the complexity and computational intensity of the LBS model. The next step of the research work is to design and implement of the privacy security model and try to solve the problem of service time extension which caused by the encryption mechanism.

Acknowledgements

This work is supported by the National Science and Technology Support Program, China (2012BAF12B19).

References

[1] W. Zhang, L. Wu, S. Liu, et al., A trajectory privacy model for radio-frequency identification system, Wireless Personal Communications 90(3)(2016) 1-14.

[2] H. Huang, T. Gong, P. Chen, R. Malekian, T. Chen, Secure two-party distance computation protocol based on privacy homomorphism and scalar product in wireless sensor networks, Tsinghua Science and Technology 21(4)(2016) 385-396.

[3] A. Ben-David, N. Nisan, B. Pinkas, FairplayMP: a system for secure multi-party computation, in: Proc. ACM Conference on Computer and Communications Security, CCS 2008.

[4] J. Li, Q. Wang, C. Wang, Fuzzy keyword search over encrypted data in cloud computing, in: Proc. the 29th IEEE International Conference on Computer Communication, INFOCOM 2010, 2010.

[5] Z. Xia, X. Wang, X. Sun, Q. Wang, A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data, Parallel & Distributed Systems 27(2)(2016) 340-352.

[6] L. Zeng, Y. Wang, D. Feng, CloudSky: a controllable data self-destruction system for untrusted cloud storage networks, in: Proc. Ieee/acm International Symposium on Cluster, Cloud and Grid Computing IEEE, 2015.

[7] S.T. Yang, M.A. Chun-Guang, C.L. Zhou, LBS-oriented location privacy protection model and scheme, Journal on Communications 35(8)(2014) 116-124.

[8] M.S.H. Talpur, M.Z.A. Bhuiyan, G. Wang, Shared-node IoT network architecture with ubiquitous homomorphic encryption for healthcare monitoring, International Journal of Embedded Systems 7(1)(2015) 43-54.

[9] Z. Montazeri, A. Houmansadr, H. Pishro-Nik, Defining perfect location privacy using anonymization, in: Proc. Conference on Information Science and Systems, 2016.

[10] F. Shirazi, M. Simeonovski, M.R. Asghar, M. Backes, C. Diaz, A Survey on Routing in Anonymous Communication Protocols, 2016.

[11] G. Xu, F. Lin, Y. Liu, An improved mix transmission algorithm for privacy-preserving, Journal of Networks 9(12)(2014) 3373-3380.

[12] F. Burgstaller, A. Derler, S. Kern, A. Reiter, Anonymous communication in the browser via onion-routing, in: Proc. International Conference on P2p, Parallel, Grid, Cloud and Internet Computing IEEE, 2015.

[13] Q. Li, H. Rong, W. Sun, J. Wang, J. Li, A correlation-based energy balanced probabilistic flooding algorithm in wireless sensor network, in: Proc. Vehicular Technology Conference (VTC Spring), 2016 IEEE 83rd, 2016.

[14] G. Retscher, T. Hecht, Investigation of location capabilities of four different smartphones for LBS navigation applications, in Proc. International Conference on Indoor Positioning and Indoor Navigation IEEE, 2013.

[15] R. Huang, X. Gui, S. Yu, Design of cloud storage framework with privacy-preserving, Journal of Xi'an Jiaotong University 45(10)(2014).

[16] G. Zhu, F. Porikli, H. Li, Tracking randomly moving objects on edge box proposals, Computer Science (2015).

[17] J. Gan, H. Xu, M. Xu, K. Tian, Y. Zhang, Y. Zhang, Study on personalized location privacy protection algorithms for continuous queries in LBS. in: Proc. Security, Privacy & Anonymity in Computation, Communication & Storage: 9th International Conference, SpaCCS 2016, 2016.

[18] Q. Yang, L.-F. Yu, X.-X. Chen, A continuous queries attacking algorithms based on fruit fly optimization method, Journal if Sichuan University (Natural Science Edition) 51(4)(2015) 725-730.

[19] P. Shanthi, S.R. Balasundaram, An efficient clique cloak algorithm for defending location-dependent attacks in location based services, in: Proc. the 2014 International Conference on Information and Communication Technology for Competitive Strategies, 2014.